Department of Justice (DOJ) Component: FBI

Total Number of Federal Employees Component-Wide: 40281

Total Number of Contract Employees Component-Wide: 6725

Department of Justice
Self-Inspection Checklist

Document Security

A. Self-Inspection Process
(Section A applies to all components)

1. Which of the following apply to your component:
(Check all that apply. If uncertain about cleared employees, request a Justice Security Tracking and Adjudication Record System [JSTARS] roster via the Compliance Review Team.)

- Create classified information — (•) Y ( ) N ( ) N/A
- Handle classified information — (•) Y ( ) N ( ) N/A
- Review classified information — (•) Y ( ) N ( ) N/A
- Store classified information — (•) Y ( ) N ( ) N/A
- Personnel do not process, handle or review classified information, but have a National Security Information (NSI)/ Sensitive Compartmented Information (SCI) clearance (Only portions of Sections E and I of the checklist apply to your component) — ( ) Y (•) N ( ) N/A
- Office does not process, handle or review classified information and no office personnel have a NSI/SCI clearance (This checklist does not apply to your component) — ( ) Y ( ) N (•) N/A

2. Does your component conduct self-inspection reviews? — ( ) Y ( ) N (•) N/A

   a. If **YES**, who is responsible for conducting the reviews?

   (U) At the FBI, Information Security Reviews are conducted by the Strategy Policy and Information Security Unit (SPISU), Mission Support Section (MSS), Security Division (SecD).

b. How is information gathered from the component Division/District/Field/Resident/Satellite/Overseas offices?

(U) SPISU conducts annual document reviews and compliance reviews of sensitive and classified information program offices across FBI field divisions.

c. Does the self-inspection include:

- Original classification assessment ○ Y ◉ N ○ N/A
- Derivative classification assessment ◉ Y ○ N ○ N/A
- Declassification assessment ○ Y ◉ N ○ N/A
- Safeguarding assessment ◉ Y ○ N ○ N/A
- Security Violations assessment ◉ Y ○ N ○ N/A
- Security Education and Training assessment ◉ Y ○ N ○ N/A
- Management and Oversight assessment ◉ Y ○ N ○ N/A
- Review of security directives and instructions ◉ Y ○ N ○ N/A
- Review of a representative sample of classified information ◉ Y ○ N ○ N/A
- Interviews with classified producers and users ○ Y ◉ N ○ N/A

d. How does your component determine which offices and activities are covered by the self-inspection?

(U) Offices chosen for review had not been inspected by either the FBI or DOJ within the last two years and had not undergone compliance reviews in the past two years.

e. How is the self-inspection data obtained from the offices (surveys, interviews, checklists, on-site inspections, etc.)?

(U) The FBI conducted onsight compliance reviews of field divisions. During the reviews, Chief Security Officers (CSOs) and their staff were interviewed and checklists were completed by the reviewers.

3. Does your component conduct compliance reviews? ◉ Y ○ N ○ N/A

a. If **YES**, what areas are reviewed?

(U) Reviews included aspects physical security, systems security, and the completion of checklists relating to the safeguarding of classified and sensitive information.

◉ Y ○ N ○ N/A

b. Are the results included in the self-inspection data call?

B. Original Classification

(Section B applies only to components with persons who have Original Classification Authority [OCA])

Note: If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

◉ Y ○ N ○ N/A

4. Do current OCAs have a demonstrable and continuing need to exercise this authority?

   a. If **YES**, please explain why OCAs have a demonstrable and continuing need.

   (U) The FBI's 17 OCAs have a demonstrable and continuing need to exercise original classification authority. OCAs compose and authorize classification guides specific to their area of subject matter expertise in order to facilitate classification decisions for the different types of information (i.e., intelligence, continuity of operations, information assurance) encountered by the FBI. Additionally, the OCAs exercise their authority to facilitate declassification decisions, to share information with Intelligence Community and law enforcement partners, and to use in legal proceedings.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

C. Derivative Classification

(Section C applies only to components with persons who reproduce, extract, or summarize classified information; or who apply classification markings derived from source material or as directed by a classification guide)

NOTE: If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

◉ Y ○ N ○ N/A

5. Do persons who apply derivative classification markings observe original classification decisions and carry classification markings forward to newly created documents?

6. Describe the process followed when derivative classifiers identify improper markings on an originally or derivatively classified document. Include actions taken or planned to correct deficiencies or misclassification actions and to deter their reoccurrence.

   (U//~~FOUO~~) Anyone who wishes to challenge the classification of FBI information may either proceed informally by directly questioning the classifier or may submit a formal classification challenge. Those who wish to challenge the classification of other

government agency (OGA) information must submit a formal classification challenge. Informal classification challenges may be invoked for derivatively classified FBI information; this includes documents marked "Classified" by an OCA or classification decisions rendered in a classification guide. All classification decisions pertaining to OGA information must be formally challenged.

(U//~~FOUO~~) Informally challenged information remains marked at the level it was originally classified but must be handled and protected at the highest level of classification of the conflicting opinions until the classification conflict is resolved.

(U//~~FOUO~~) When uncertainties exist over the classification status of derivatively classified information, holders of this information are encouraged to make direct contact with the derivative classifier to correct the classification prior to making a formal classification challenge. Informal classification challenges do not require intervention by SecD. However, challengers may make an informal request to SPISU for guidance and resources to help resolve the dispute.

(U//~~FOUO~~) When approaching a derivative classifier with a classification challenge, the challenger should be prepared to justify the challenge by referencing an OCA's classification determination as conveyed in a classification guide or a properly, accurately marked source document. After the challenger approaches the derivative classifier who originated the document or information, the derivative classifier may either accept the proposed classification correction or determine that the information should remain marked as is.

(U//~~FOUO~~) If the derivative classifier accepts the proposed classification correction, he must create a record copy of the corrected document and, to the most practical extent, notify all holders of the information that the corrected document must be used instead of the incorrectly classified document. The derivative classifier must also record the change, to include the derivative source for the classification, and maintain a record of the change with the file or record copy of the document.

(U//~~FOUO~~) If the derivative classifier determines that the information should remain marked as is, the individual who challenged the classification may not change the marking on the originator's document. If the individual who challenged the classification still believes the information is incorrectly classified and wants to ensure that the correct markings are placed on the originator's document, the individual can then can initiate a formal classification challenge.

(U//~~FOUO~~) Formal classification challenges may be invoked for both originally and derivatively classified information, regardless of agency of origination. Formal challenges are made by filling out the "FBI Formal Classification Challenge Form FD-1061" and submitting it to SPISU. This submission may be either electronic or hard copy. All attempts will be made to resolve challenges within 60 days of receipt by SPISU. If unable to resolve the challenge within 60 days, SPISU will acknowledge the

challenge in writing and provide a revised resolution date. The written response will also advise that if a response is not provided within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision.

(U//~~FOUO~~) For challenges to derivatively classified information, SPISU will determine the appropriate classification guide(s) and respective OCA(s) associated with the information. Then, SPISU will liaise with that OCA (or the subject matter expert designee) to determine the proper marking for the information. All decisions and historical information pertaining to the challenge will be recorded by SPISU.

(U//~~FOUO~~) For challenges to originally classified information, SPISU will liaise with the OCA who made the decision, as well as any other applicable OCAs (or their subject matter expert designee), to determine the proper classification of the information. The OCA who originally classified the information in question will make the final classification decision.

(U//~~FOUO~~) For challenges to the classification of information originated an OGA, SPISU will liaise with the proper point of contact to determine proper classification of the information. All decisions and historical information pertaining to the challenge will be recorded by SPISU and a final classification decision will be rendered and conveyed. To close the review, SPISU will complete the FBI Formal Classification Challenge Form FD-1061.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

D. Classified Markings Review
(Regular reviews of representative samples of the component's original and derivative classification actions shall be conducted in accordance with **32 CFR Part 2001, Section 2001.60[c][2]** to evaluate the classification and marking of the documents and electronic communications. These samples must encompass all component activities that generate classified information.)

7. How often is sampling of original and derivative classification actions reviewed? (If **Other**, please explain.)
   ○ Monthly ○ Semi-annually ◉ Annually ○ Other ○ N/A

   Click here to enter text.

   a. Identify what factors are considered in establishing time frame.

      (U) All documents that were reviewed were created within fiscal year (FY) 2014. The FBI reviewed an assortment of electronic communications (ECs), emails, and

intelligence information reports. Every document reviewed was classified at the confidential or secret level. The reviews ensured that basic requirements (i.e., banner line, portion marking, classification blocks, and foreign dissemination markings) were met. Reviewers did not challenge the classification level of portions, instead deferring to the author's subject matter expertise unless the portion was blatantly over classified. If a document was marked as multiple sources it was noted and the source was noted as present; however, this was not part of overall criteria for analysis.

8. Identify total number reviewed as a representative sample. A specific number must be provided for the various items reviewed:

   - Originally classified hard copy documents
     0
   - Originally classified e-mails
     0
   - Derivatively classified hard copy documents
     330
   - Derivatively classified e-mails
     71

   a. Do the representative sample reviews encompass all agency activities that generate classified information? ◉ Y ○ N ○ N/A

      a.1. If **YES**, list the various types of formats reviewed, e.g., internal e-mails, external e-mails, bulletins, electronic communications, reports, presentation slides, cables

      (U) The FBI reviewed classified investigative documents including but not limited to letterhead memoranda, ECs, Sentinel import forms, and emails.

   b. Are classified documents properly marked in accordance with the Information Security Oversight Office December 2010, Marking Classified National Security Information Marking Book or agency specific marking guide? ◉ Y ○ N ○ N/A

   c. Identify number of classified items sampled where discrepancies were noted. A specific number must be provided for the various items reviewed:

      - Originally classified hard copy documents
        - List the specific formats identified with the discrepancies
        - List the specific types of discrepancies identified **(see Attachment 1)**

(U) During the review period, the FBI had no originally classified hard copy documents.

(U) The following issues were identified:
- Incorrect portion marks
- Missing portion marks
- Incorrect declassification dates
- Improper format of banner line
- Citation of multiple sources that were not listed
- Entirely wrong classification block

- Originally classified e-mails
  - List the specific formats identified with the discrepancies
  - List the specific types of discrepancies identified **(see Attachment 1)**

(U) During the review period, the FBI had no originally classified emails.

- Derivatively classified hard copy documents
  - List the specific formats identified with the discrepancies
  - List the specific types of discrepancies identified **(see Attachment 1)**

Click here to enter text

- Derivatively classified e-mails
  - List the specific formats identified with the discrepancies
  - List the specific types of discrepancies identified

Click here to enter text.

d. Describe actions taken or planned to correct the discrepancies identified above

(U) The primary cause of the referenced discrepancies falls into two categories:

(U) Classification Management Tool (CMT) – The CMT is deployed on several FBI platforms, including Microsoft Applications (e.g., Outlook) and Sentinel. Currently, there are inconsistencies among versions of the CMT since there are multiple versions of the CMT running across the enterprise. SecD is working with Information Technology Engineering Division to ensure the same updated version of the CMT is deployed throughout the FBI.

(U) User Errors – To reduce and mitigate errors, the FBI continued to provide training awareness on correct classification marking and handling procedures to all FBI personnel. The FBI has developed and launched web-based training for designating, marking, and handling classified information. Every document reviewed was classified at the confidential or secret level.

(U) In FY 2013, the FBI published five security bulletings. Security bulletins are intended to notify FBI personnel of newly-available resources, such as the publication of a new classification guide, or to provide awareness of common marking errors in order to correct problematic trends.

e. What **percentage** of derivatively classified **hard copy** actions reviewed contained derivative classifier's name and position, or personal identifier?
18%

f. What **percentage** of derivatively classified **e-mail** actions reviewed contained derivative classifier's name and position, or personal identifier?
100%

g. How many derivatively classified **hard copy** actions reviewed were derived from multiple sources?
0%

g.1 What **percentage** of the documents had a list of sources included or attached?
0%

h. How many derivatively classified **e-mail** actions reviewed were derived from multiple sources?
0%

h.1 What **percentage** of the e-mails had a list of sources included or attached?
0%

i. How does your component ensure the material reviewed provide a representative sample of classified information?

(U) The FBI reviewed a random selection of documents. In the review, a pattern was identified to indicate that there were specific categories of errors present in all reviewed FBI documents. The errors can be attributed to errors in the CMT, user errors, and training gaps.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section.

(U) The only original classification decisions made by the FBI during the reporting period were updating classification guides. Therefore, there were no emails or other communications to be reviewed.

(U) The FBI did not review any hardcopy documents. All documents were in electronic format and were drawn from the FBI Intranet Intelligence Portal, Sentinel, or emails received by the reviewer over the course of FY 2014. In the event there was a citation of multiple sources, a notation was made but the FBI did not analyze an error rate associated with this particular error.

E. Security Education
NOTE. If SEPS provides the services for your component, a comment box is provided at the end of the section for further elaboration.

(OCAs are required to receive training in proper classification and declassification each calendar year.)

9. How many OCAs exist within the component? 17
   a. What **percentage** of OCAs received initial OCA training prior to originally classifying information? 100%

   b. What **percentage** of OCAs have received annual OCA refresher training?
   100%

   c. Have any waivers to this requirement been granted?
   0

(Derivative classifiers are required to receive training in the proper application of the derivative classification principles of EO 13526 each calendar year. SEPS considers a derivative classifier as anyone with a clearance because the employee has the potential to access and derive classified information. If your component does not concur with SEPS' approach please provide a reason and a list of individuals considered derivative classifiers.)

10. How many derivative classifiers exist within the component?
    47,006

    a. What **percentage** of derivative classifiers have received initial derivative classification training prior to derivatively classifying information?
       100%

    b. What **percentage** of derivative classifiers have received annual refresher training?
       92.4%

    c. Have any waivers to this requirement been granted?
       No

(All cleared personnel are required to receive initial training on basic security policies, principles, practices; and criminal, civil, and administrative penalties. Agencies are required to provide annual refresher training to all employees who create, process, or handle classified information [NSI/SCI]. Cleared personnel who leave the Department or whose clearance has been administratively withdrawn or revoked are required to receive a termination briefing.)

11. How many cleared federal employees exist within the component?
    40,281

    a. What **percentage** of cleared federal employees receive initial training?
       100%

    b. What **percentage** of cleared federal employees receive refresher training?
       92.4%

12. How many cleared federal employees left the Department or had a clearance administratively withdrawn or revoked in the past year?
    1724

    a. What **percentage** of these cleared federal employees received a termination briefing?
       100%

13. Are authorized couriers of classified information briefed on their responsibilities? ◉ Y ○ N ○ N/A

14. Are records kept of the various training and briefings provided (initial/refresher/termination/courier) and the employees who participated? ◉ Y ○ N ○ N/A

15. How many cleared contract employees exist within the component world-wide?
6725

a. Who is responsible for providing contract employee training and briefings (initial/refresher/termination/courier)?

(U) The FBI CSO of the field or Headquarters division where the employee is assigned is responsible for providing entry and exit briefings of all FBI employees.

b. If DOJ is responsible for providing the contractor training and briefings, list the training and briefings provided and how often they occur.
N/A

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

F. Declassification
(Section F applies only to components that create/maintain classified permanent records designated as such through an approved records schedule.)
NOTE. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

16. Does your component create or maintain classified permanent records designated as such through an approved records schedule? ◉ Y ○ N ○ N/A

17. Describe the process and procedures for how your component accomplishes declassification reviews of your classified permanent records. If your component works directly with SEPS to assist with your automatic declassification reviews, please state in your response.

(U) The FBI's approach to automatic declassification is to first evaluate information at the file series level. File series exemptions are sought for those file series that are

national security related and the oldest information in the file series is at least 25 years old. When a file series exemption is granted, the information undergoes a review pursuant to the systematic declassification review provisions of Executive Order 13526 (see answer 18a). Classified FBI information residing in non-national security related file series (or other file series that do meet the criteria for a file series exemption) is automatically declassified without review when the information reaches 25 years of age.

18. Do Interagency Security Classification Appeals Panel (ISCAP) approved exemptions or file-series exemptions apply to classified permanent records your component creates or maintains? ◉ Y ○ N ○ N/A

a. If **YES**, describe the process and procedures for how your component accomplishes systematic reviews of your exempt classified permanent records. If your component works directly with SEPS to assist with your systemic declassification reviews, please state in your response.

(U) The FBI's Record/Information Dissemination Section (RIDS) is responsible for declassification reviews under the systematic declassification provisions of Executive Order 13526. While conducting these reviews, RIDS ensures information which no longer meets the criteria for classification established by the FBI Automatic Declassification Guide (ADG) is declassified and information that continues to meet the criteria for exemption from automatic declassification remains classified. The FBI's ADG contains a list of exempt file series that require systematic review. In prioritizing the review of each exempt file series, RIDS considers factors such as the following: expiration date of the exemption, the size of the file series in relation to the expiration date of the exemption, historical significance, the organizational priorities of the Records Management Division and FBI Executive Management, and priorities established by the National Declassification Center.

(U) During systematic declassification reviews each classified record is evaluated using the following process:

- Determine the originator of the classified information: Classified information that originates with another agency is tabbed using a Standard Form 715 to indicate that the information must be forwarded to the originating agency, which then makes a classification determination.
- Determine the age of the information: When FBI classified information is aged at least 25 years but less than 50 years, the exemption codes lised in the ADG are eligible for application. At this time, RIDS reviewers will determine whether the classified information under review fits into any of the specified exemption codes.

Classified information which, pursuant ot the ADG, is exempt from automatic declassification is tabbed using a Standard Form 715 to indicate the exempt status of the information. Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from automatic declassification is declassified. When the FBI classified information is aged 50 years or older, the review is limited to an evaluation as to whether the information is eligible for exemption from automatic declassification pursuant to portions of the ADG that implement Section 3.3(h)(2) of Executive Order 13526. There are only three categories of information that can be considered for exemption from automatic declassification at 50 years: 1) the identity of a confidential human source or human intelligence source, 2) key design concepts of weapons of mass destruction, and 3) "extraordinary cases." Classified information which, pursuant to the ADG, is exempt from automatic declassification at 50 years is tabbed using a Standard Form 715 to indicate the exempt status of the information. Classified information which, pursuant to the ADG, no longer meets the criteria for exemption from declassification is declassified.

19. Describe your component's procedures for mandatory declassification review requests received from the public.
(Mandatory declassification review requests apply to both classified permanent and temporary records. If you are unfamiliar with mandatory declassification reviews, contact your Freedom of Information Act [FOIA] section as they are usually the section that would initially receive these requests.)

(U) The following procedures are followed upon receipt of a MDR request from the public:

- Data about the request is entered into the RIDS electronic case management and redaction system (FDPS).
- Using the criteria established in Executive Order 13526 and its implementing directives, the request is reviewed to determine whether it is a valid MDR. If the MDR is not valid, RIDS will provide the requester with, in writing, the reason(s) for the denial of the MDR and an opportunity to modify the request or provide more information in order for the request to be processed. Additionally, RIDS will notify the requester of the right to appeal the denial decision.
- Upon verification that RIDS is in receipt of a valid MDR, a search is conducted for records containing the information sought in the request. If no record is found, the requester is advised of this fact in writing and the requester is advised of his right to appeal this determination.

- When responsive records are located, RIDS performs a line-by-line declassification review of the information in accordance with applicable executive orders, regulations, policies, classification guides, or declassification guides. When information responsive to a MDR request originates with another agency and is in the possession of the FBI, RIDS will refer the information and the request letter to that agency. The receiving agency will communicate its determinations to RIDS. Then, RIDS will incorporate the other agency determinations into a final determination.
- For information that RIDS approves for declassification, RIDS will mark or redact the information appropriately in FDPS to clearly designate that the information has been declassified. When information cannot be declassified in full, RIDS will make reasonable efforts to release those portions of requested information that constitute a coherent segment.
- Once the declassification review is complete, RIDS performs a separate line-by-line review for public release purposes, including a review to identify information that is exempt from disclosure under the provisions of a statutory authority, such as but not limited to the Freedom of Information Act (FOIA).
- The requester is then provided with the responsive documents and/or the reason(s) why information is being withheld or redacted, including citations to sections 1.4 or 3.3 of Executive Order 13526 or other specific legal authority. The requester is also notified of his appeal rights.

20. Does your component have a process for facilitating public release or access of declassified documents, e.g., FOIA Electronic Reading Rooms, FBI Vault? ◉ Y ○ N ○ N/A

    a. If **YES**, please describe the process.

    (U) The mission of RIDS is to effectively plan, develop, direct, and manage responses to requests for access to FBI records and information. The requests and disclosures comply with the Freedom of Information and Privacy Acts (FOIPA), Title 5, United States Code, Sections 552 and 552a; the MDR and systematic review provisions of Executive Order 13526; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and other Presidential and Congressional directives.

    (U) RIDS efforts are directed to appropriately release information in an efficient and effective manner while protecting legitimate law enforcement, foreign policy, national security, and defense interests.

    (U) To date in FY 2014, the FBI has received over 17,500 FOIPA and other access requests from the public. Pursuant to these requests, RIDS has reviewed at least

1,100,000 pages. These requests, including FOIPA-related requests, are processed in an electronic case management and redaction system (i.e., FDPS) which promotes the efficient processing and release of declassified non-exempt information to the public. In late FY 2013 a new version of FDPS was deployed which allowed for even more efficient processing and disclosure of declassified non-exempt information to the public in FY 2014. During FY 2014, FDPS was continuously enhanced with additional features to further the goal of efficient FOIA processing. RIDS can respond to requesters in either paper or electronic formats.

(U) To facilitate public access to declassified and other non-exempt information, RIDS maintains a public website known as "The Vault." Thus far in FY 2014, "The Vault" has received more than 4,500,000 views. The website contains approximately 3.8 terabytes of historically significant information on more than 500 different subject matters. The accessibility of information on "The Vault" continues to receive a significant amount of positive feedback from the requester community, the media, and the general public.

(U) Additionally, thus far in FY 2014, RIDS has conducted declassification reviews on more than 700,00 pages of permanently valuable classified records aged 25 years and older pursuant to the systematic declassification provisions of Executive Order 13526. Nearly all of these pages will be transferred to the National Archives where they will undergo further processing for eventual availability to the public.

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

G. Safeguarding

NOTE. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

21. Is all classified material properly protected in accordance with 32 CFR Part 2001, Subpart D and the DOJ Security Program Operating Manual (SPOM), Chapter 6?

- Do you have a system of control measures which assures access to classified information is limited to authorized persons? ◉ Y ○ N ○ N/A
- Do you have a system of control measures which deter and detect access by unauthorized persons? ◉ Y ○ N ○ N/A
- Is classified material stored in General Services Administration (GSA)-approved security containers or Department Security Officer (DSO) approved open storage areas? ◉ Y ○ N ○ N/A
- Is Top Secret information stored in a GSA-approved security container along with proper supplemental controls? ◉ Y ○ N ○ N/A
- Are combinations safeguarded the same as the highest level of classified information being protected? ◉ Y ○ N ○ N/A
- Are combinations changed only by persons authorized access to the highest level of information stored in the container? ◉ Y ○ N ○ N/A
- Do you use Standard Form (SF) 700s "Security Container Information"? ◉ Y ○ N ○ N/A
- Is classified information kept under constant surveillance and covered to prevent unauthorized access when removed from storage for working purposes? ◉ Y ○ N ○ N/A
- Is system of security checks or inspection implemented at the close of each business day to ensure classified information is properly secured? ◉ Y ○ N ○ N/A
  - Are SF 702s "Security Container Check Sheets" utilized? ◉ Y ○ N ○ N/A
  - Are SF 701s "Activity Security Checklist" utilized? ◉ Y ○ N ○ N/A
- Does the official responsible for arranging a conference or meeting institute ensure adequate security is proved if classified information is to be discussed? ◉ Y ○ N ○ N/A

- Are meetings held only in a U.S. Government facility or at a cleared facility of a DOJ contractor or consultant? ◉ Y ○ N ○ N/A

- Are attendees notified of imposed security limitations due to attendees' access level authorizations or physical security conditions of the facility? ◉ Y ○ N ○ N/A

22. Is all classified material transmitted in accordance with 32 CFR Part 2001, Section 2001.45 and the DOJ SPOM, Chapter 6-500? ◉ Y ○ N ○ N/A

    - Is classified information physically transmitted outside the facility in two opaque layers? ◉ Y ○ N ○ N/A

    - Is authorization to hand-carry classified information between DOJ components and other organizations only given to DOJ personnel appropriately briefed and authorized in writing by the SPM? ◉ Y ○ N ○ N/A

23. Is all classified material reproduction in accordance with 32 CFR Part 2001, Section 2001.44 and the DOJ SPOM, Chapter 6-402? ◉ Y ○ N ○ N/A

    - Held to a minimum consistent with operational requirements? ◉ Y ○ N ○ N/A

    - Accomplished only by authorized persons knowledgeable of the procedures for classified reproduction? ◉ Y ○ N ○ N/A

    - Accomplished only with approved equipment? ◉ Y ○ N ○ N/A

    - Appropriate procedures for reproduction of classified information posted on or near equipment approved for such reproduction? ◉ Y ○ N ○ N/A

24. Is all classified material destroyed in accordance with 32 CFR Part 2001, Section 200.46 and the DOJ SPOM, Chapter 6-600? ◉ Y ○ N ○ N/A

If **NO** to **21-24**, please explain further. **Click here to enter text.**

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

H. Telecommunications, Automated Information Systems (IT) and Network Security
NOTE. If SEPS provides the services for your component, a comment box is provided at the end of the section for further elaboration.

25. Do all IT systems that process, store, or handle classified information meet the requirements in the DOJ SPOM, Chapter 8? ◉ Y ○ N ○ N/A

    a. If **NO**, please explain.
    Click here to enter text.

26. Are all IT system components having the potential to retain classified information marked with the highest classification level and most restrictive classification category?

    a. If **NO**, please explain.
    Click here to enter text.

27. Is all data introduced on a classified IT system the same or lower security classification level for which the IT system is approved to operate? ◉ Y ○ N ○ N/A

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.
Click here to enter text.

I. Security Violations
(All security violations are required to be reported to the DSO.)

28. Is the loss, possible compromise, or unauthorized disclosure of classified information appropriately reported in accordance with the DOJ SPOM, Chapter 1-300? ◉ Y ○ N ○ N/A

    a. Are personnel familiar with the reporting procedures? ◉ Y ○ N ○ N/A

    b. What procedures are implemented to conduct an inquiry/investigation?

(U) In accordance with the FBI's Corporate Policy Directive 0610D, personnel who have knowledge of the loss, possible compromise or unauthorized disclosure of classified, NSI, PII, FTI, or Sensitive but Unclassified information are required to report the circumstances to their security office. Security personnel must then notify the Security Compliance Unit (SCU), MSS, Security Division, who oversees and manages the FBI's Security Incident Program. Personnel also have the option to report a security violation by filing a report in the Security Incident Reporting System (SIRS). Upon receipt, SCU ensures that all incidents are appropriately documented, investigated, and mitigated; all incidents are managed via SIRS from inception to completion. To ensure all security concerns are resolved, SCU works closely with CSOs who are charged with the responsibility to conduct an inquiry into each incident that occurs within their division.

c. Are appropriate and prompt corrective actions taken when a security violation or infraction occurs? Describe the process.

(U) Yes. SIRS is the FBI's central database used to capture all security incidents reported by employees and personnel associated with the FBI. Upon receipt of an incident, SCU personnel work with CSOs, security professionals, or other entities as needed to ensure the incident is properly investigated and mitigated. In addition, all parties that may have a vested interest in reported security incidents are notified. For example, referrals may be made to the following entities:

- Initial Processing Unit, Inspection Division - potential misconduct
- Privacy & Civil Liberties Unit, Office Of General Counsel - potential breach of personally identifiable information
- Counterintelligence Division - potential espionage matters
- Enterprise Security Operations Center, SecD - information technology incidents
- SPISU: Federal taxpayer information and information security incidents

(U) As part of the mitigation of incidents, CSOs also conduct awareness briefings and/or provide training on security policy and procedures to individuals who commit security incidents.

d. Are individuals who commit violation or infractions subject to appropriate sanctions? ◉ Y ○ N ○ N/A

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. Click here to enter text.

J. Management and Oversight

NOTE. If SEPS provides the services for your component, N/A will apply to that particular question. A comment box is provided at the end of the section for further elaboration.

29. How many personnel are dedicated to manage the classified national security information program? 13

30. Are sufficient resources and personnel committed to implement the classified national security information program? ○ Y ◉ N ○ N/A
If **NO**, please explain.

(U) More dedicated personnel and funding for travel are required to provide more customized training across the FBI's 56 field divisions and Headquarters. The current restrictions on traveling to field divisions limits SecD's ability to conduct thorough onsite reviews and self inspections of the FBI's classification management capabilities. The restrictions also prevent SecD from providing crucial, in-depth training to field personnel. Furthermore, this limits the FBI's ability to conduct thorough document reviews.

(The performance contract or other rating system of OCAs, security managers, and other personnel whose duties significantly involve the creation or handling of classified information must include a critical element to be evaluated relating to designation and management of classified information. "Significantly" is defined as an individual who has access to a classified network.)

31. How many personnel fit within the categories identified above? 100%

    a. What **percentage** of such personnel at your component has this element in their performance contracts? 100%

EXPLANATORY COMMENTS: Use the space below to elaborate on questions within this section. For example, if SEPS handles any of these services for your component please indicate the level of involvement and types of services provided.

All FBI employees currently have a critical element (CE) item in their Performance Plan that holds the employee accountable for their performance and management of classified information in accordance with Executive Order 13526, 5.4(d)(7) and DOJ SPOM Chapter 6, Section 11. The FBI's Performance Appraisal System currently holds employees accountable for properly handling classified information through the "Maintaining High Professional Standards" CE. Specifically, one of the bullets under this performance standard states "tasks will be completed in compliance with applicable laws, regulations, and policies." Any employee who improperly handles classified information is accountable under the applicable standard for the aforementioned CE in his Performance Appraisal Report. Due to the nature of their positions, certain FBI employees (e.g., CSOs and Assistant CSOs) have specific bullets intended to identify and address compliance with handling classified information in the "Achieving Results" Addendum of their Performance Plans. There is no immediate need for a CE to Performance Plans, as

employees are effectively held accountable for the handling of classified information.

In addition, SecD holds all FBI enforces the notion of employee accountability for the handling of classified information through the following training requirements: Annual Security Awareness Training; Annual Information Security Training; Annual Classified Marking Training. Additional training on protecting, handling, and transporting classified informaotin is held with individual field and Headquarters divisions. Lastly, SecD provides and tracks briefings for individuals responsible for transporting classified information.

Please include the following information in your report to the DSO on the results of your self-inspection:

1. Provide best practices that were identified during self-inspections.

   (U) The FBI uses a multi-layered approach of training awareness to address information security trends and identification of errors through both incident reporting and annual reviews. In addition to the required annual Information Security (INFOSEC) Course, the FBI has created a web-based referesher National Security Information Marking and Handling Course, which is mandatory for all users of FBI systems. In FY 2014, the FBI has also launched a Working with National Security Information Course, which is offered for FBI personnel with the need for in-depth training. This training provides updates on rules, as well as practice marking more complex classified information.

   (U) The FBI has created a Marking Classified information 2.0 class for the advanced users of classified information. This training has been provided on an ad hoc basis to the field and upon request for analytical and investigative personnel across the FBI. In addition, the FBI has completed the second cycle of using a web based training as the "refresher" training for all users of FBI IT Systems. The FBI is the only component of the DOJ that is currently using the CMT to mark classified information. Over 22 FBI IT systems are using a marking tool to mark classified information. The CMT correctly formats a banner line and portion marks on classified documents. It is the goal of the FBI to have all FBI systems using the same version of the CMT to ensure current marking standards and rules are applied.

ATTACHMENT 1
EXPLANATION OF DISCREPANCIES

OVERCLASSIFICATION: (a) Clear-cut: The information in the document does not meet the standards necessary for classification; (b) Questionable: While the question of meeting classification standards is arguable, classification does not appear to be necessary to protect our national security; (c) Partial: A portion(s) of the document appear(s) to be unnecessarily classified, although the overall classification of the document is correct.

OVERGRADED: All or some of the information in the document appears to be classified at a higher level than justified.

UNDERGRADED: All or some of the information in the document appears to be classified at a lower level than necessary.

DECLASSIFICATION: The document has improper or incomplete declassification instructions or no declassification instructions.

The "Declassify on" line should contain one of the following:
(1) a date or event less than 10 years from the date the information/document was created;
(2) a date 10 years from the date the information/document was created;
(3) a date greater than 10 years and less than 25 years from the date the information/document was created;
(4) a date 25 years from the date the information/document was created;
(5) 25X1–25X9, with a date or event of declassification, provided that the classifying agency has received approval from the Interagency Security Classification Appeals Panel (ISCAP) to exempt the information;
(6) 50X1–50X9, with a date or event of declassification, provided that the classifying agency has received approval from the ISCAP to exempt the information;
(7) 50X1-HUM or 50X2-WMD, provided that the ISCAP has been informed of the agency's intent to use this marking; or
(8) 25X1, E.O. 12951, provided that the document contains space-based imagery.

Other markings, such as "OADR" and X1–X8, are not valid under the current Order, and "MR," "DCI/DNI Only," and "Subject to International Treaty or Agreement" have never have been valid declassification markings. See 32 C.F.R. Part 2001 and/or the ISOO booklet, "Marking Classified National Security Information," for further details.

When declassification dates are displayed numerically, the following format must be used: YYYYMMDD.

DURATION: A lesser duration of classification appears more reasonable.

UNAUTHORIZED CLASSIFIER (Unknown Basis for Classification): The document appears to have been classified by someone not authorized to do so.

"CLASSIFIED BY" LINE – Original Classification (Unknown Basis for Classification): The document does not identify the OCA by name and position or by personal identifier. If the identification of the originating agency or office is not apparent on the face of the document, it should be listed below the position.

"REASON" LINE: An originally classified document does not include the "Reason for Classification," or it cites an incorrect category from section 1.4 of the Order. A "Reason" line does not appear on a derivatively classified document, and if included is cited as a discrepancy.

"CLASSIFIED BY" LINE – Derivative Classification (Unknown Basis for Classification): The document does not identify the derivative classifier by name and position or by personal identifier.

ATTACHMENT 1
EXPLANATION OF DISCREPANCIES

"DERIVED FROM" LINE (Unknown Basis for Classification): The document fails to cite, or cites improperly, the classification source. The line should include type of document, date of document, subject, and office/agency of origin.

MULTIPLE SOURCES(Unknown Basis for Classification): The document cites "Multiple Sources" as the basis for classification, but does not list these sources.

ORIGINAL/DERIVATIVE: The document is marked and treated as an original classification action although the classified information appears to be derived from a guide or other source(s).

MARKING: The document lacks overall classification markings or has improper overall classification markings (e.g., lacks the highest overall marking, contains erroneous overall markings, or lacks overall markings and/or caveats on transmittal documents).

PORTION MARKING: The document lacks required portion markings.